IT Faculty
Cyber security

ICAEW INFORMATION TECHNOLOGY FACULTY

2016
ICAEW.COM/ITFAC

10 STEPS TO CYBER SECURITY FOR SMALLER FIRMS

INFORMATION TECHNOLOGY FACULTY

10 steps to online security for SMEs

THE TEAM

George Quigley
Chairman
T: +44 (0)20 7893 2522
E: george.quigley@kpmg.co.uk

Jeremy Boss
Deputy chairman
T: +44 (0)7791 293 319
E: jeremy.boss@btinternet.com

Richard Anning
Head of IT Faculty
T: +44 (0)20 7920 8635
E: richard.anning@icaew.com

Kirstin Gillon
Technical manager
T: +44 (0)20 7920 8538
E: kirstin.gillon@icaew.com

Mark Taylor
Technical manager
0207 920 8476
Mark.Taylor@icaew.com

David Lyford-Smith
Technical manager
020 7920 8643
David.Lyford-Smith@icaew.com

Tracy Gray
Services manager
T: +44 (0)20 7920 8526
E: tracy.gray@icaew.com

Contact details
IT Faculty
ICAEW
Chartered Accountants' Hall
Moorgate Place
London EC2R 6EA UK
+44 (0)20 7920 8481
itfac@icaew.com
icaew.com/itfac

Cyber Security is produced by Progressive Customer Publishing
71-73 Carter Lane
London
EC4Y 0AN

Advertising enquiries to
advertising@progressivecp.com

To comment on your magazine, please email us at publishing@icaew.com

Printed in the UK by Pensord

Since we issued the first edition of 10 steps to cyber security in 2013, much has changed. But the central issue of how to protect yourself, your firm and your clients from cyber-attack remains the same.

And the backdrop is a world in which criminals are getting ever more inventive and successful. In the faculty we have spent time working with members, industry experts and government to understand the issues, inform our thinking and provide advice and guidance to members.

Over the period we have run a series of roundtables with security professionals, FTSE 100 board directors, and members in small businesses and practices. In the larger businesses it was felt there was a disconnect and lack of a meaningful conversation between the business and the IT/security team. In smaller businesses it was felt that there was not sufficient time available to spend on proper security (which we considered really translated to a lack of priority given).

We worked with the government in the creation and launch of the Cyber Essentials scheme (which was launched by the minister in Chartered Accountants' Hall back in June 2014). This is the base level that is designed to demonstrate good basic cyber hygiene and help improve the chances of avoiding a cyber-attack by as much as 80%. Of note, ICAEW gained Cyber Essentials certification in 2015.

Following meetings with and feedback from members, we worked with the Department for Business, Innovation and Skills (BIS) to create a free, interactive online training course aimed at finance professionals. Taking an hour to complete, the course is aimed at helping members to understand the issues and feel more confident when talking with colleagues, suppliers and clients.

Over the past three years we have produced a series of reports outlining the findings of the top six audit firms based on their interaction with clients. *Audit Insights: Cyber Security* outlines four flags boards should be aware of and charts a widening gap between the capabilities of businesses and those of the cyber-criminals. For more information, visit icaew.com/auditinsights

We continue to track upcoming legislation, noting recent directives and regulation that may affect members. Advice on this and all of our output is available to members online at our Cyber Resource Centre at icaew.com/cyber.

We welcome your feedback on our work, as well as any questions or suggestions you may have on what else we can do to support ICAEW members.

Richard Anning
Head of faculty

ILLUSTRATIONS: ERIC FROMMELT/IKON

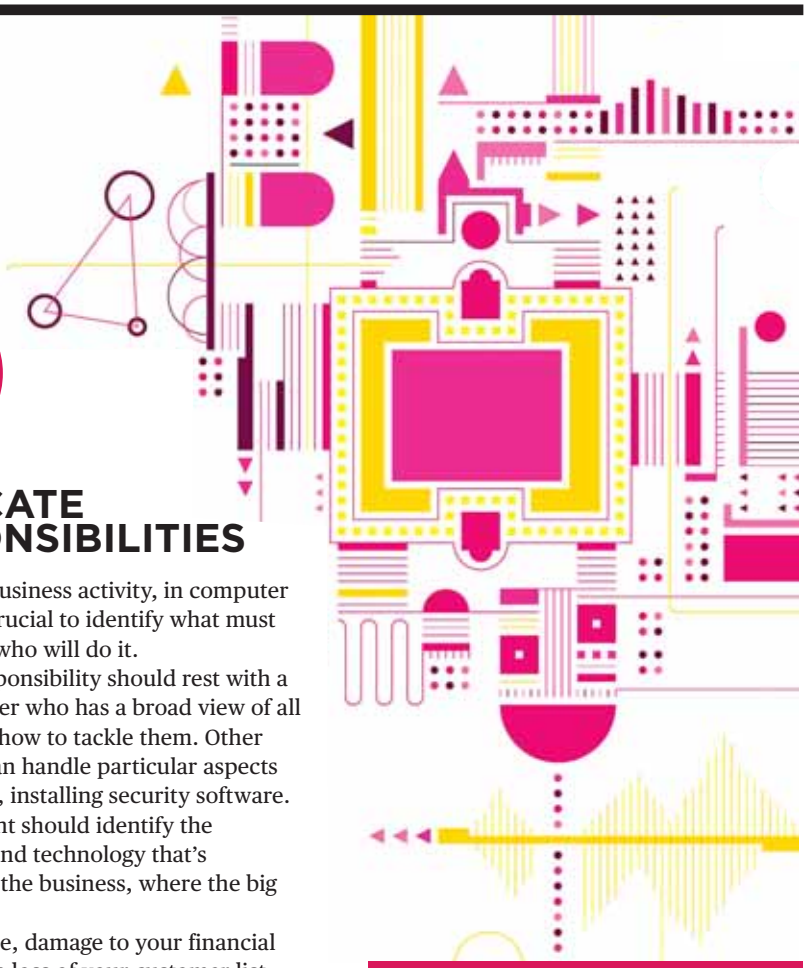
10 STEPS TO ONLINE SECURITY FOR SMES

Following these basic steps will improve your chances of avoiding an online attack by as much as

80%*

1. Allocate responsibilities
2. Protect your computers and your network
3. Keep your computers up to date
4. Control employee access to computers and documents
5. Protect against viruses
6. Extend security beyond the office
7. Don't forget disks and drives
8. Plan for the worst
9. Educate your team
10. Keep records - and test your security

*AS OUTLINED BY GCHQ IN THE 10 STEPS TO CYBER SECURITY



1

ALLOCATE RESPONSIBILITIES

As with any business activity, in computer security it's crucial to identify what must be done and who will do it.

Overall responsibility should rest with a senior manager who has a broad view of all the risks and how to tackle them. Other individuals can handle particular aspects - for instance, installing security software.

Management should identify the information and technology that's really vital to the business, where the big risks lie.

For example, damage to your financial system, or the loss of your customer list, could lead to the failure of the business. Other information may be less important.

Equally, some computers are probably more critical, or more vulnerable, then others. Identifying the risks, then establishing what security measures already exist and whether they work, and what extra ones are required, will help you to target your security efforts where they are most needed.

BUYING SECURITY

While many large organisations need security consultants, smaller businesses can be protected by security software. Usually, only basic knowledge is required to install it. Built-in (default) settings provide essential protection, although remember to change default passwords. More expertise might be needed for advanced features.

2

PROTECT YOUR COMPUTERS AND NETWORK

Malicious activity could come from outside or inside your business.

Attacks from outside, for example by troublemaking hackers or competitors, can be protected against by installing a firewall. This is software or hardware which examines all the computer communications flowing in and out of the business, and decides whether it's safe to let them through.

It can also be used to manage your staff's internet activity, for instance by blocking access to chat sites where employees might encounter security risks. You can set up (configure) the firewall to allow or prevent certain kinds of activity.

There are several different kinds of firewall. The router supplied by your Internet service provider (ISP) may already have one built-in, or you can buy a software firewall solution.

Protecting against illicit activity from inside the business requires other precautions we'll look at elswhere in this supplement. All of these also provide extra protection against attacks from outside.

3 KEEP YOUR COMPUTERS AND DEVICES UP TO DATE

Suppliers of PCs, software, and operating systems such as Windows frequently issue software updates (patches) to fix minor problems (bugs) or improve security.

It's essential to keep all your computers and other devices up-to-date with the latest patches. Normally, they can be downloaded and installed automatically.

Remember that just one vulnerable computer puts all the others at risk. It's important to ensure that all available patches are applied to all of them.

SMART PASSWORDS

Passwords should be difficult to guess but memorable, and never written down. Some hackers employ 'dictionary attacks' which try every possible word until they find the right password. You can protect against this by ensuring that passwords include a combination of upper- and lower-case letters, numbers and symbols. Require employees to change passwords regularly. Security software may be able to expire them after a set period, so that they have to be changed.

5 PROTECT AGAINST VIRUSES

Malicious software or 'malware' (a category including viruses, Trojans and spyware) may not always be as devastating as the headlines suggest, but can still slow down your systems dramatically, and passing them on to customers will win you no friends.

Fortunately, there is plenty of protection available. Your computers may have been sold with anti-virus software (the generic term, although most products also protect against other kinds of malware). If not, you can easily buy it.

This software regularly scans a computer in search of malware, deleting any that is found.

Regular updates to head off new threats are key to anti-virus software. So this is one area where it does pay to stick to the big brand names and to ensure that the software is set to receive updates as regularly as possible (ideally daily).

4 CONTROL EMPLOYEE ACCESS TO COMPUTERS AND DOCUMENTS

Although your computers should be guarded by a firewall, you should still protect user accounts (each person's 'identity' with which they log on to a computer) and sensitive documents with passwords.

Because each individual should have a unique user name and a password, access to different parts of your IT can be limited to certain people. (Some individuals may have more than one user name and password, perhaps if they have multiple roles.)

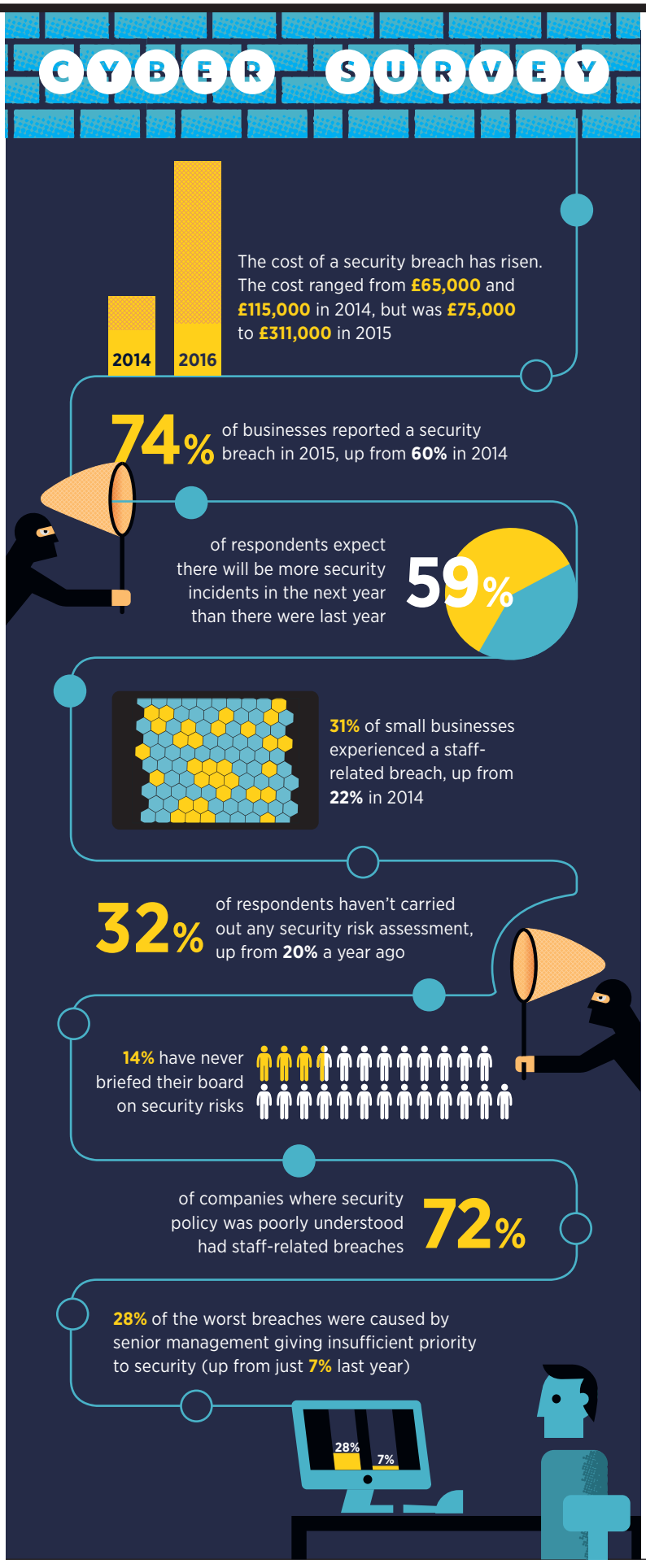
This not only protects against accidental or intentional damage by staff to systems and information, it also provides further security against outside intrusions.

To achieve this, you can use security options built in to operating systems such as Windows, or you can buy specialised software online.

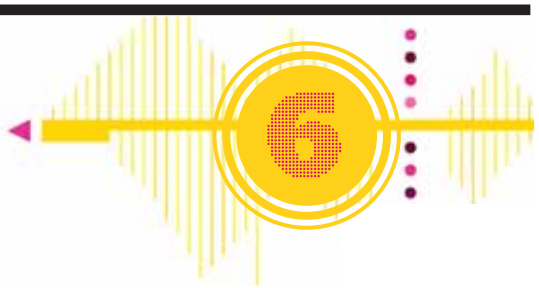
Because you identified your biggest security risks and most vital information in Step 1, you can decide whether password control for a given item should be basic (for instance, one password authorising access to an entire computer) or stronger (each document or application requiring a separate password).

Some individuals designated as computer administrators (admins) may be given access to nearly everything, in order to perform technical work. You should keep the number of admins to a minimum.

Security software will usually generate records showing which employees have used particular computers or documents at different times. This can be useful for pinpointing problems, but access to these records should, of course, be tightly limited - otherwise people misusing the system could alter them to cover their tracks.



BIS RECEIVED 664 SURVEY RESPONSES TO THE 2015 BREACHES SURVEY, FROM ALL INDUSTRY SECTORS



EXTEND SECURITY BEYOND THE OFFICE

Today's employees often work from home or on the road using their own laptops, phones and tablets. It is difficult to extend the same level of security you can apply to office computers to these devices. But you can reduce risk by requiring any personal equipment used for work is approved.

It should have the minimum of anti-virus software, password protection and (where applicable) a firewall. And to protect against unauthorised access to information when a device is mislaid or stolen, it should be possible to delete all the information ("wipe" it) even when you don't have the device. This capability is built into newer models; software can also be bought to perform remote wiping, but this must be installed before the device is lost.

Ensuring the sensitive data is kept in an encrypted area (see section 7) of the computer or device will stop most attempts to access data. This is easy to set up using off-the-shelf software. Beware of the dangers when connecting to unencrypted public wifi, as hackers can intercept data. Check the hotspot is genuine and make sure file sharing is off and the firewall is on.

SAFETY IN THE CLOUD

More and more businesses are using cloud computing, where software is provided and documents are stored by a specialist company accessed via the internet, rather than on your own computers. This brings security considerations, though not necessarily extra risk.

You should ensure that your cloud computing provider takes security measures at least equal to those of your own business. They'll probably be better, but do ask detailed questions, and remember that if the provider is in another country, legal requirements may be different.

REMEMBER DISKS AND DRIVES

Removable disks and drives such as DVDs and USB sticks pose security risks in two ways. They can introduce malware into your computers, and they can be mislaid when containing sensitive information.

Ensure that as far as possible, only disks and drives owned by your business are used with your computers. Discourage employees from using them in third parties' computers (in Internet cafes for example), and set up anti-malware software to scan them whenever they are used in the office.

Establish a routine to track who has possession of each disk or drive at any given time, and check that all documents are erased from them after use.

ENCRYPTION

Sensitive information can be encrypted for further security. Encryption transforms the contents of documents into apparently random sequences of characters, which can only be turned back into meaningful information when users enter a password (the key) or plug in a special device (a dongle).

WHY DOES IT MATTER TO ME AS A SMALL BUSINESS?

All the information within a company has a value, not just to that company but also to their competitors, organised crime, commercially or politically motivated hackers and others. You might be surprised what other people would find valuable, and no business is too small to be a target. If it's valuable to anyone, it's at risk. Of course, as soon as you start working with other organisations, you will also have a responsibility for protecting their data too. Cyber incidents, including malicious or accidental data loss, can bring about huge financial burdens to a business, with direct financial losses estimatedat £75,200 to £311,000 for small businesses.

Information Commissioner's Office (ICO) fines of up to £500,000 can also be levied if a business breaches the Data Protection Act.

No security can be 100% effective. People make mistakes, equipment fails and the threats keep changing. However, the threats are real for small and large business alike and are not going away. The simple steps outlined in this booklet will help protect against many of the common, low level cyber threats. If a company can apply these steps, it will help protect their own, their partners' and their customers' data.

Dr Emma Philpott, CEO The IASME Consortium

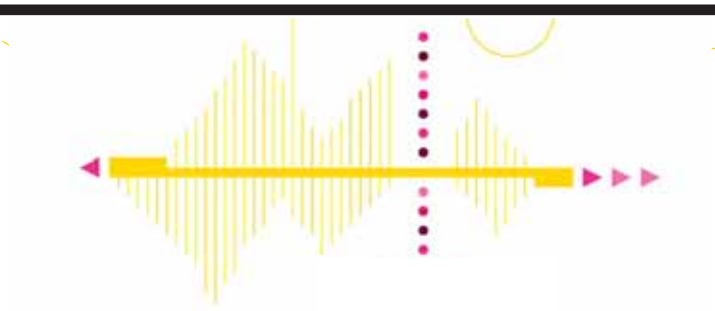
WHY DOES IT MATTER TO SMALL PRACTICES?

"We don't hold banking details of our clients; our data is of no interest to a hacker." This is a sentiment I have come across a number of times in client meetings. My reaction is simple, I take a USB stick out of my pocket, hand it across the table to them and ask for a copy of all the data held in the organisation.

After an initial bemused reaction and a polite refusal to my request, I ask what data they have that they would not want to willingly hand over to me. This then starts the thought processes going. Perhaps they run a payroll and might be worried if salary details of clients got out of the building. Perhaps they file tax returns and accounts on behalf of their clients which need to be kept confidential. Perhaps they have other personal details of their clients they would not want divulged – or details of a financial transaction they are involved with. The list can actually be quite long.

If a small practice would be unwilling to hand over all their organisation's data to me on a USB stick, why would they run the risk of handing them over to competitors, troublemakers or irresponsible employees inadvertently through an online breach or a careless error? It is important to understand your critical data assets and take care to protect them, online as well as off. Following the simple steps in this guide will help you to reduce your risk and strengthen the service you can offer to your clients.

George Quigley, chairman IT Faculty and KPMG partner



8 PLAN FOR THE WORST

Following the measures in this guide will help you protect against a major security breach. But no system is 100% secure, so it's worth planning what you'd do if things went badly wrong.

First, define what is 'major' for you. Something that puts a non-critical department of the business offline for a couple of hours probably isn't. But something that prevents you serving customers, or performing vital functions such as payroll, will be.

Establish how you will know that there's a problem. You shouldn't have to wait for computers to go down; your firewall or anti-virus software, for example, may provide advance warning that something unusual is going on.

Plan your next steps. What help (perhaps a specialist computer company) should you call in? Do you need to contact key customers or suppliers to explain that there is a problem? Can some functions be continued using other computers, or pen and paper, while your systems are repaired?

Finally, ensure that it's clear who is responsible for doing what in an emergency. Your plan can be laid out in a document, and delivered in training sessions. It may incorporate elements of your plans for other disasters, such as a fire on your premises, and cut-down versions can be applied to less damaging computer incidents.

9 EDUCATE YOUR TEAM

Tell everyone in the business why security matters, and how they can help, using training sessions and written policy documents. This will encourage them to follow practices such as regular password changes.

Most will not have to actively work at security. They'll simply need to be aware of risks - for example, knowing that they should never click on a web link or attachment in an email from an unfamiliar source.

There are non-technical risks, too. One is social engineering, where hackers try to trick employees into revealing technical details that make your computers vulnerable. For example, a hacker might pretend to work for your computer supplier and claim they need passwords to perform maintenance.

The casual atmosphere of social media such as Facebook could be conducive to such deceptions, so employees should be especially wary of discussing your systems and practices on social media.

DON'T PANIC

Security matters, but it is also important that team members do not become so paralysed by fear that they – and your business – lose out on the many benefits of the online world, or even reject contact with potential customers. Sensible caution is often better than absolute bans.

10 KEEP RECORDS AND TEST YOUR SECURITY

Security is an ongoing process, not a one-off fix. So it's important to keep clear records. For example, the decision- making in Step 1 of this guide could help you produce a list of all your hardware and software, along with an indication of how secure each item needs to be.

Similarly, records of software patches and lists of authorised personal devices will help build up a picture of your business's security status, spot potential weak points, and figure out how any problems arose.

Good record keeping will also help you regularly test all your security measures, and ensure that you have functioning, up-to-date software. Any business is only as secure as its weakest link, and testing will make sure that no weaknesses are overlooked.

USEFUL LINKS

The faculty resource centre icaew.com/cyber

Cyber security: what small businesses need to know – advice from BIS gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

Information Commissioners Office ico.org.uk

Get Safe Online Getsafeonline.org/businesses

An essential guide to security standards

Navigating the expanding landscape of information security standards can be a challenge. So if you don't know your PCI DSS from your ISO 27001, Lesley Meall's at-a-glance guide can help

As computing and communication devices, software, data and networks have become more accessible and prolific, their security has become more complex. So has the landscape of information security frameworks, schemes and standards. The occupants now include (but are not restricted to) COBIT, Cyber Essentials, PCI DSS and the ISO/ICE 27000 series. It's almost enough to make you hanker for the mainframe or desktop computing eras, when you could draw a bright line around your IT assets and their security.

Well, almost. A more connected and ubiquitous computing ecosystem is not without benefits. But technologies and trends such as cloud computing, growing (personal and professional) use of mobile devices and social media, and the emergence of 'big data' have created new and significant security challenges. Very few organisations are now immune to vulnerabilities, such as leaky employee endpoints, as well as threats and risks, such as disruption to business, fines and reputational damage.

"The threat from IT security breaches is too significant for accountants with IT roles to overlook the information security frameworks, schemes and standards that can help to identify, assess and address the key risks and threats," says Omer Tariq, manager for risk and advisory at BDO. Marc Vael, international vice president at the Information Systems Audit and Control Association (ISACA), a professional association focused on IT governance adds: "Understanding them can help you to save valuable time building proper information security in your organisation and when validating and confirming where you are with this."

Figuring out how much you need to understand in order to do this is almost as complex as some of the standards. Among the many potential influences are:

- where your responsibilities for IT security begin and end;
- the size, type and structure of your department or organisation;
- ownership and use of IT assets, products and services;
- IT management and governance frameworks in use;
- existing IT security policies and procedures;
- compliance with statutory, sector and supplier requirements; and
- access to technical expertise and financial resources.

So your need to know (as an individual, department or organisation) will sit somewhere on a very broad spectrum - not unlike the information security responsibilities and technical expertise of the members of the IT Faculty. But everyone has to start somewhere, and if you don't already know your COBIT from your PCI DSS, or your ISO 27001 from your BS7799-2, a basic grasp of some of the most widely used frameworks, schemes and standards relating to IT security is an important step on the road to enlightenment - or certification.

Let's begin with the latest and greatest UK government initiatives in this area, and see where this leads. us.

CYBER ESSENTIALS SCHEME

This is a key objective of the National Cyber Security Strategy and is being delivered as part of the government's National Cyber Security Programme.

Since 1 October 2014, the UK government has required all suppliers bidding for certain personal and sensitive information handling contracts to be Cyber Essentials (CE) certified. Any other business can choose to be certified.

You can learn more about cyber essentials requirements, the assurance framework that underpins the assessment, approved accreditation bodies that certify companies to provide CE services, the two available levels of CE certification and how to get hold of them at cyberstreetwise.com/cyberessentials

The CE scheme focuses on the most common internet-based cyber security threats. However, its requirements reflect longer-established and more extensive IT security standards, such as the ISO/IEC 27000 series.

ISO/IEC 27000 SERIES

This started life as a 1980s government initiative by the Commercial Computer Security Centre of the now defunct Department of Trade and Industry; then, after a long and circuitous international journey, the 27000 series of information standards was launched in 2005 (learn more at 27000.org/thepast.htm), to help organisations improve their information security management.

The members of this fledgling family of standards you are most likely to encounter are 27001 and 27002.

27001 provides the requirements for establishing, implementing, maintaining and continuously improving an information security management system (ISMS); it replaced the BS7799-2 standard.

27002 outlines the hundreds of potential controls and control mechanisms, which may be implemented subject to the guidance in 27001. 27002 superseded ISO 17799 standard (a code of practice for information security).

You can learn more about the development of other standards in the 27000 series at 27000.org/contact.htm and find out about other ISO standards related to the 27000 series at 27000.org/other.htm

Numbers in the ISO 27000 series (also known as the ISMS family of standards) are allocated by the International Organisation for Standardisation (ISO, iso.org) which has developed and published more than 19,500 voluntary 'best practice' standards. ISO is a membership network of national standard setters, such as the UK British Standards Institution (BSI) – a private company incorporated by Royal Charter.

There is no law that says you have to comply with 27001 or gain certification for this, and some organisations choose to implement the standard (or part of it) just for the benefits it brings. But as compliance with 27001 is required of product and service providers to an increasing number of businesses and government bodies (across the globe), some organisations need to implement it and to demonstrate this – which is possible only with the help of an independent accredited certification provider. ISO advice on selecting a certification body/provider is at iso.org/iso/home/standards/certification.htm, and a flowchart showing the ISO 27001 certification process is at 27000.org/ismsprocess.htm

Finding organisations that can provide 'independent' ISO 27001 certification is as simple as Googling 'iso 27001 accredited certification providers', which brings up possibilities ranging from the Big Four accounting firms to specialists such as BSI (and yes, that is the same BSI that acts as the UK's national standard setter).

> No law says you have to comply with 27001, but compliance with 27001 is required of product and service providers to an increasing number of businesses

IASME STANDARD

The IASME Consortium created the Information Assurance Management Standard for SMEs in 2013. It offers small businesses an option that is less challenging to achieve and maintain than ISO 270001; a high-level comparison of the four standards is available at iasme.co.uk/index.php/about/iso

The IASME Consortium Ltd is one of two bodies currently accredited to appoint Cyber Essentials certification providers. IASME evolved from another government initiative, and took forward a project of the Technology Strategy Board, a non-departmental public body, established by the government in 2004, and funded by the Department for Business, Innovation & Skills (BIS).

You can learn about approaches to certification, including companies that are licensed to deliver IASME assessments and routes to becoming an assessor, by visiting the website, **iasme.co.uk/index.php/become-an-assessor**

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. PCI DSS is different to Cyber Essentials, the ISO 27000 series, the IASME standard and COBIT in one very significant way: compliance is not optional, though it's not a statutory requirement.

Merchants who do not comply with PCI DSS can find themselves held responsible for any losses incurred through fraud and face fines from the acquiring bank or financial institution that they use to process card payments – and almost all merchants who take card payments are expected to meet one of the four levels of PCI DSS compliance.

You can learn more about why and how to become compliant at pcisecuritystandards.org and find companies and providers that are qualified to provide PCI DSS-related products and services at pcisecuritystandards.org/approved_companies_providers/index.php

For a a jargon-free version of the website for merchants running small outlets is available at pcisecuritystandards.org/smb/

COBIT

Control Objectives for Information and Related Technology (COBIT) is an IT governance framework, with a supporting toolset. It defines a set of generic processes that can be used by business managers, IT professionals and assurance professionals to enable good practice and policy development for IT governance and control throughout an organisation.

The global non-profit organisation ISACA first released COBIT in 1996. It's a high-level business oriented framework, so it is not focused solely on IT security or internet-based cyber security, though many organisations use COBIT as the framework for their governance and control systems. In 2013, ISACA released the guidance Transforming Cybersecurity Using COBIT 5 (the latest version, which incorporates the ISACA risk IT framework and the ISACA Business Model for Information Security).

In 2013 ISACA also launched the COBIT 5 Certified Assessor Program to recognise professionals with the skills to perform COBIT-based IT process assessments and the necessary experience in planning, building, running and/or monitoring IT processes, and provide them with a credential.

You can learn more at isaca.org

Lesley Meall is a freelance writer and ex-software engineer. She is author of the *Chartech* guides to online accounting software, using dashboard software, and payroll software and services

SPOILED FOR CHOICE?

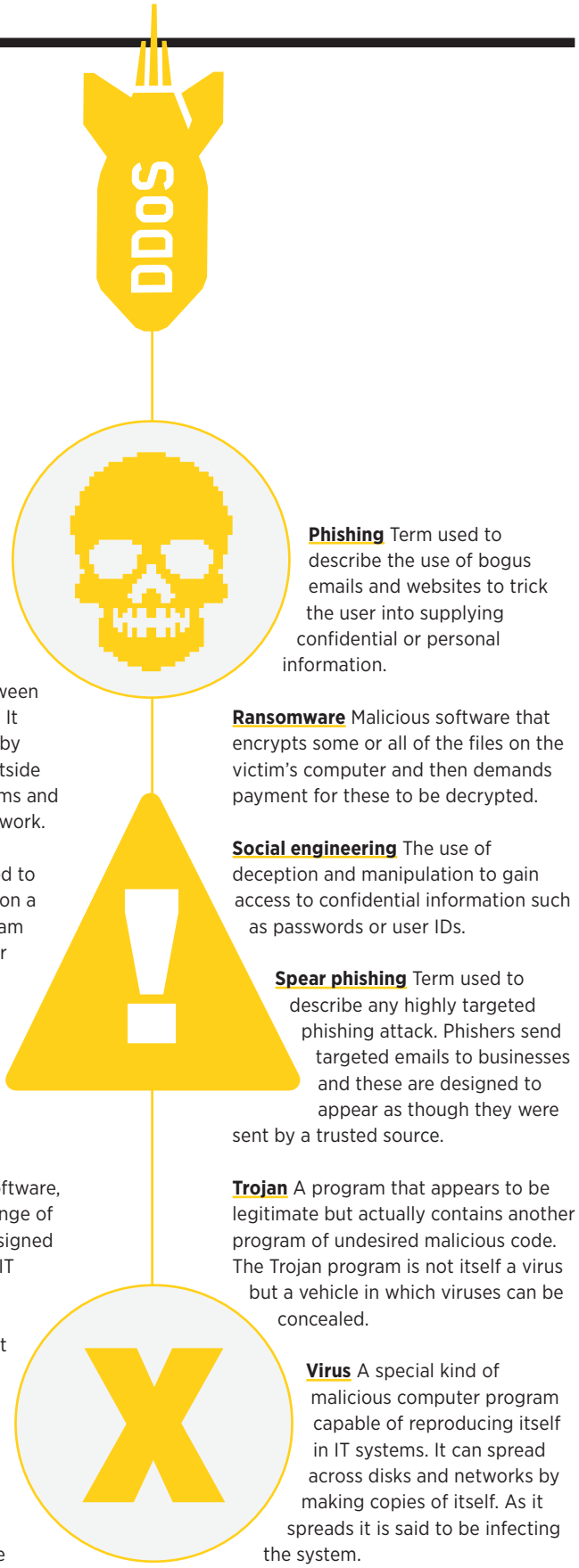
The schemes, standards and frameworks covered here are just some of the many out there. Different countries have their own equivalent to the UK Cyber Essentials scheme (such as the National Institute of Standards and Technology Cybersecurity Framework in the US); even a single organisation such as the ISO has many standards relating to information security (not just the 27000 series). It can be hard to see beyond the hyperbole of service providers with vested interests and there is no consensus on which individual or combined approach is superior.

A user of COBIT may also need to demonstrate compliance with the Cyber Essentials scheme, PCI DSS and ISO 27001, despite overlaps; another organisation may need to comply with PCI DSS and Cyber Essentials, while compliance with 27001 or COBIT could be overkill.

As ISACA's Vael says, "all of the frameworks, schemes and standards should be considered as good inspiration sources. But all of them require intelligent interpretation". So although this *Chartech* article may be enough to help some accountants with IT roles or responsibilities to assess their options, identify the standards and certifications that might best meet their needs, and form the basis of any necessary action, for others it may be one small step on a long and winding road through a landscape – and where some of you find a lot more investigatory work lies head.

Who knows what it all means?

Some IT security terms can be confusing. So here we explain some of the most commonly used jargon to help you get started



Breach In a security context this term is used to describe an act from outside the organisation that bypasses the existing security defences and results in the unauthorised access of data, applications or services.

Brute force attack An attempt to decode security passwords or encryption keys by sequentially testing them against every possible permutation password rather than employing a more 'scientific' approach

Cyber security An overarching term used to describe the measures taken to protect IT systems from unauthorised access or manipulation.

Data leakage/loss Term used to describe the deliberate or accidental release of sensitive corporate data, commonly relating to finances, customers, intellectual property and other confidential information. The term has become more commonplace with the growing use of mobile devices that pose increasing security risks.

(Distributed) Denial of service attack (DDoS) The intention of such an attack is to deny access to a website, usually as a result of the implementation of malicious procedures by hackers. Denial of service is achieved by attacking network components, such as routers and computer systems. The result is a website ceasing operation until the problems are resolved.

Encryption The translation of data into a secret code that cannot be easily understood by an unauthorised person. Encryption has become particularly important in wireless communications, mobile devices and memory sticks.

Firewall A hardware or software security device that filters information passing between internal and external networks. It controls access to the internet by internal users, and prevents outside parties gaining access to systems and information on the internal network.

Key logger A program designed to record which keys are pressed on a computer keyboard. The program records each keystroke the user types and uploads the information to whoever installed the program. This information may contain details of passwords, usernames and online banking services.

Malware Short for malicious software, a generic term that covers a range of software programs that are designed to attack, degrade or infiltrate IT systems.

Password/pass phrase A secret series of characters that enables an authorised user to gain access to a file, computer or program. It is important that users are encouraged to set strong passwords as poorly set passwords can compromise the security of the computer system. The use of a multi word pass phrase is preferred over a simple password. These are easier for people to remember and harder for computers to guess.

Phishing Term used to describe the use of bogus emails and websites to trick the user into supplying confidential or personal information.

Ransomware Malicious software that encrypts some or all of the files on the victim's computer and then demands payment for these to be decrypted.

Social engineering The use of deception and manipulation to gain access to confidential information such as passwords or user IDs.

Spear phishing Term used to describe any highly targeted phishing attack. Phishers send targeted emails to businesses and these are designed to appear as though they were sent by a trusted source.

Trojan A program that appears to be legitimate but actually contains another program of undesired malicious code. The Trojan program is not itself a virus but a vehicle in which viruses can be concealed.

Virus A special kind of malicious computer program capable of reproducing itself in IT systems. It can spread across disks and networks by making copies of itself. As it spreads it is said to be infecting the system.

An extended version of this glossary can be found in the Cyber Resource Centre. For more information, visit icaew.com/cyber

Making IT work for you

If you are an accountant in practice or in business, we will keep you up-to-date with technology issues and developments to help you make the best possible use of IT.

Features and benefits of membership

- ***Chartech:*** bi-monthly magazine containing news, articles and case studies.
- **Publications:** technical information in simple, easily digested formats.
- **Excel Community:** now including two suites of Excel online training – standard and advanced.
- **Webinars:** freely available to faculty members on a range of tech and Excel topics.
- **IT Counts:** an online community where you can share up-to-the-minute tech news and views.
- **Thought leadership:** working in the public interest to improve IT in the profession.
- **Career development:** resources to support your continuing professional development.

Join the IT Faculty today to receive a comprehensive and accessible package of guidance and technical advice to help you stay ahead of the rest.

Twitter.com/icaew_ITFaculty

Linkedin.com – find ICAEW

ICAEW INFORMATION TECHNOLOGY FACULTY

BUSINESS WITH CONFIDENCE

icaew.com/itf